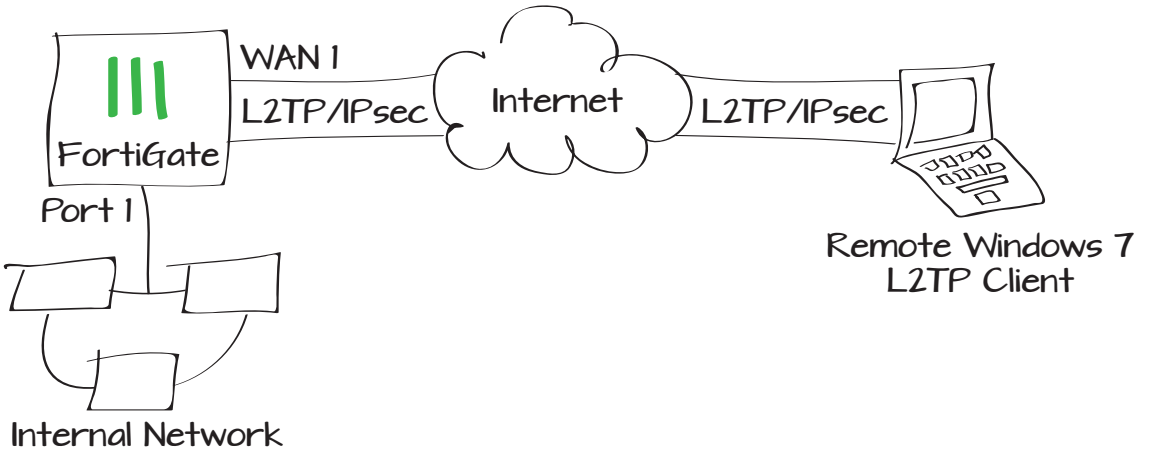
Configuring a FortiGate unit as an L2TP/IPsec server

The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP/IPsec tunnel with the FortiGate unit directly. Creating an L2TP/IPsec tunnel allows remote users to connect to a private computer network in order to securely access their resources. For the tunnel to work you must configure a remote client to connect using an L2TP/IPsec VPN connection. This recipe is designed to work with a remote Windows 7 L2TP client.

The FortiGate unit must be operating in NAT/Route mode and have a static public IP address.

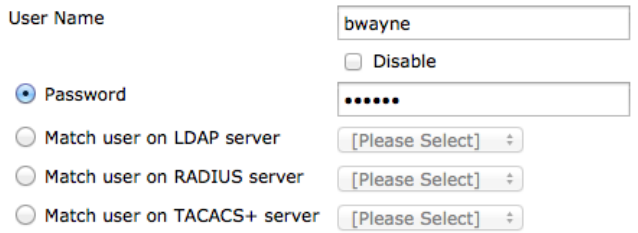
1. Creating an L2TP user and user group
2. Enabling L2TP on the FortiGate
3. Configuring the L2TP/IPsec phases
4. Creating security policies for access to the internal network and the Internet
5. Configuring a remote Windows 7 L2TP client
6. Results



Creating an L2TP user and user group

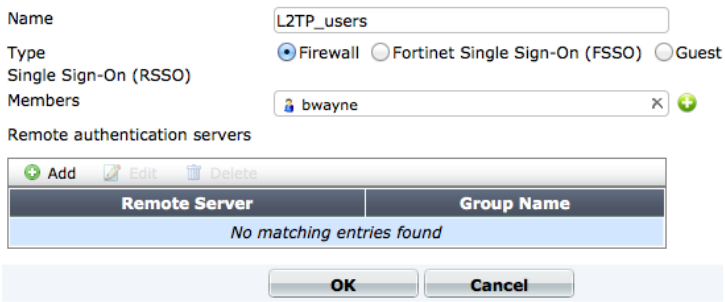
Go to **User & Device > User > User Definition**.

Create a new L2TP user for each remote client.



Go to **User & Device > User > User Groups**.

Create a user group for L2TP users and add the users you created.



Enabling L2TP on the FortiGate

Enable L2TP on the FortiGate and assign an IP range for L2TP users.

Go to **System > Dashboard > Status > CLI Console** and enter the CLI commands shown here.

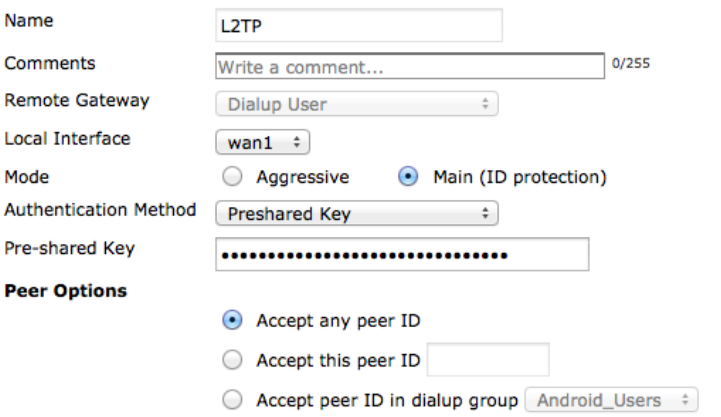
The **sip** indicates the starting IP in the IP range. The **eip** indicates the ending IP in the IP range.

```
config vpn L2TP
     set sip 192.168.10.1
     set eip 192.168.10.101
     set status enable
     set usrgrp L2TP_users
end
```

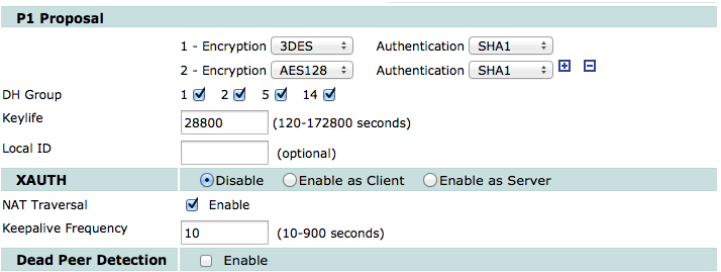
Configuring the L2TP/IPsec phases

On the FortiGate, go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the FortiGate, **Local Interface** to the Internet-facing interface, and enter a **Pre-shared Key**.

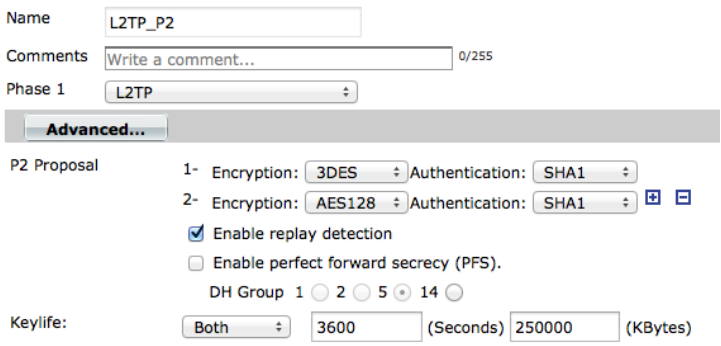


Enable all of the **DH Groups** and disable **Dead Peer Detection**.



When you are finished with Phase 1, select **Create Phase 2**. Name it appropriately and set it to use the new L2TP Phase 1.

Expand the **Advanced** options and specify a suitable **Keylife**. For example, **3600** seconds and **250000** KBytes.



Go to **System > Dashboard > Status > CLI Console**. In the **CLI Console** widget, edit the Phase 2 encapsulation mode using the CLI commands shown here.

```
config vpn ipsec phase2
     edit L2TP_P2
          set encapsulation transport-mode
end
```

Creating security policies for access to the internal network and the Internet

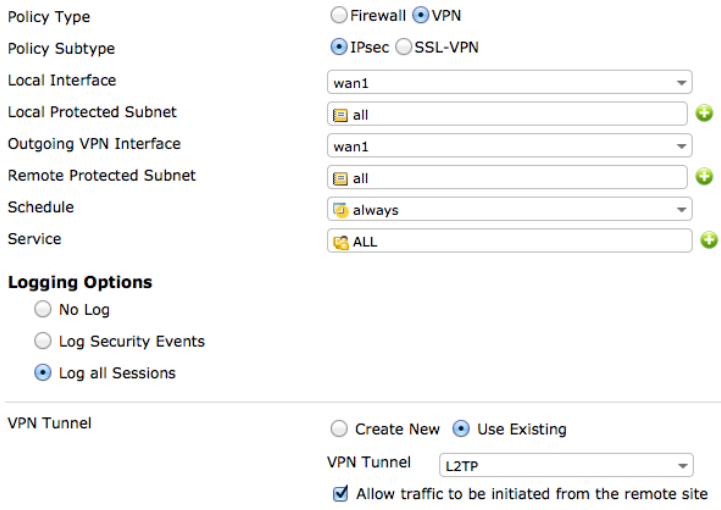
To ensure that policy-based IPsec VPN is enabled, go to **System > Config > Features,** turn on **Policy-based IPsec VPN**, and click **Apply**.

Go to **Policy > Policy > Policy**.

Create an **IPsec VPN** security policy to allow inbound and outbound traffic on wan1 by setting both the **Local Interface** and the **Outgoing VPN Interface** to **wan1**.

Set both the **Local Protected Subnet** and the **Remote Protected Subnet** to **all**.

Next to **VPN Tunnel**, select **L2TP** and **Allow traffic to be initiated from the remote site**.



Go to **Policy > Policy > Policy**.

Create a **Firewall** security policy allowing remote L2TP users access to the internal network.

Set the **Incoming Interface** to **wan1** and the **Outgoing Interface** to **internal**.

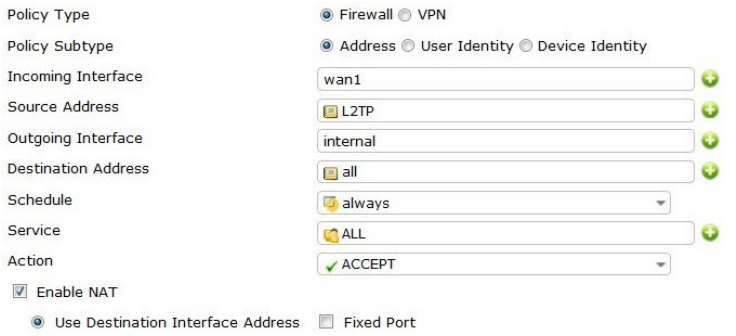
Set the **Source Address** to the L2TP tunnel range.

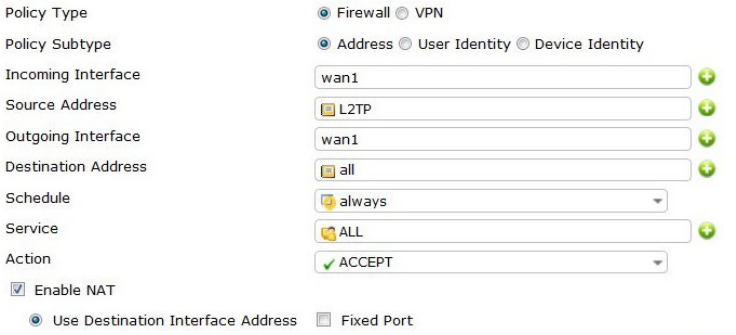
Go to **Policy > Policy > Policy**.

Create another **Firewall** security policy allowing **wan1** to **wan1** traffic so that clients connected with L2TP can access the Internet through the VPN.

Set the **Incoming Interface** to **wan1** and the **Outgoing Interface** to **wan1**.

Set the **Source Address** to the L2TP tunnel range.



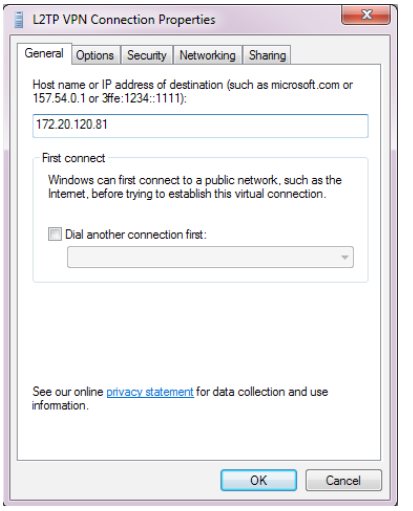


Configuring a remote Windows 7 L2TP client

To connect to the FortiGate using L2TP, the remote client must be configured for L2TP/IPsec. The following configuration was tested on a PC running Windows 7.

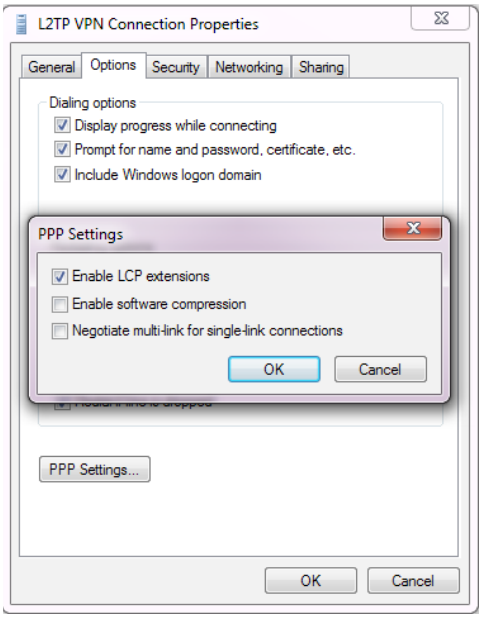
On the Windows PC, create a new VPN connection.

Right-click on the new connection and select **Properties**, then modify the connection with the settings shown.



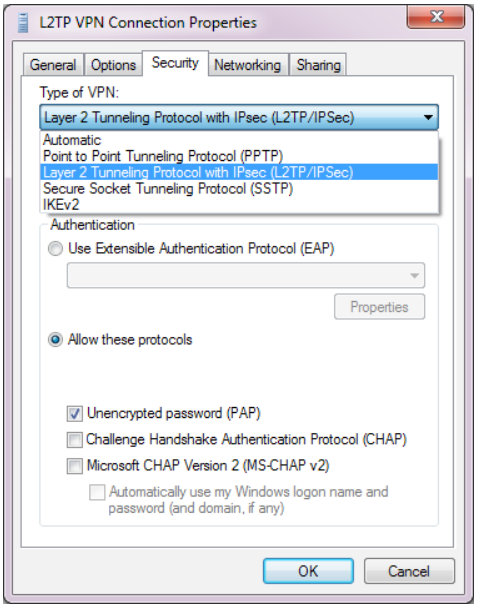
The **Host name** is the wan1 interface of the FortiGate unit that is acting as the L2TP/IPsec server.

Under the **Options** tab, enable **LCP extensions**.

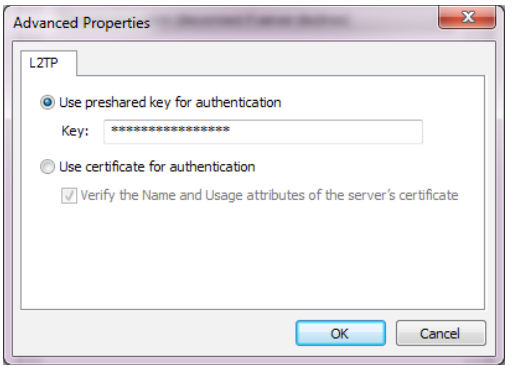


Under the **Security** tab, set the **Type of VPN** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**.

Ensure that you allow only **Unencrypted password (PAP)** protocol. Disable other protocols.



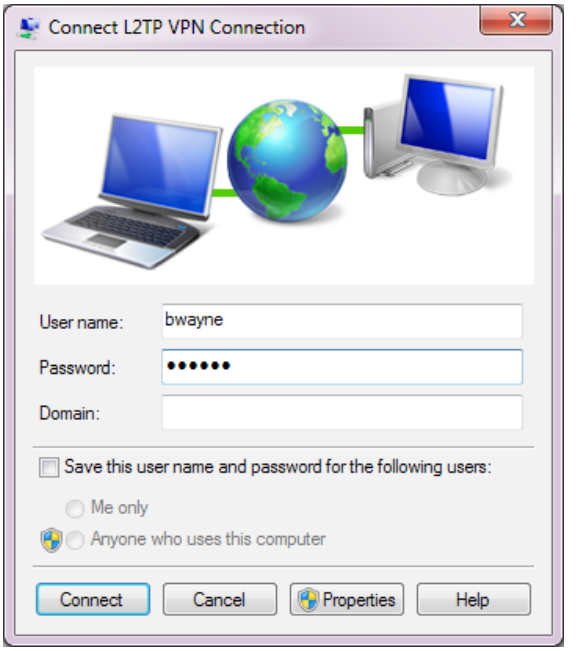
Click **Advanced Settings** and enter the pre-shared key you created in the Phase 1 configuration on the FortiGate.



Results

On the remote user's PC, connect to the Internet using the L2TP/IPsec connection you created.

Enter the L2TP user's credentials and click **Connect**.

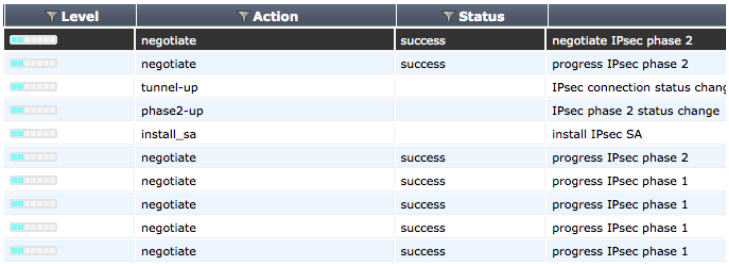


Verify the connection in the GUI by navigating to **VPN > Monitor > IPsec Monitor**.

You can view more detailed information in the event log. Go to **Log & Report > Event Log > VPN**.

Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source
L2TP_0	Dialup	172.20.120.222	0		3584	172.20.120.81-172.20.120.81

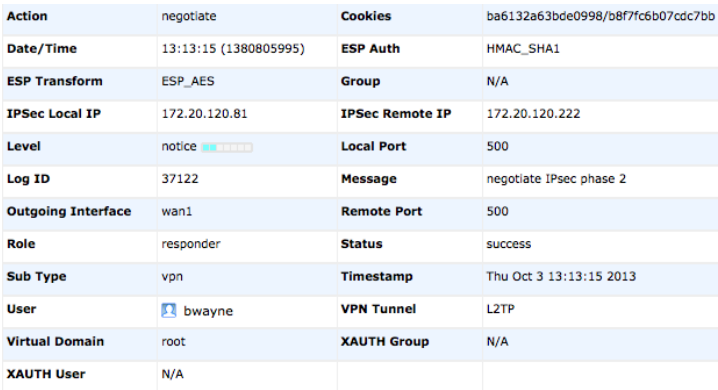
Proxy ID Destination	Status	Incoming Data	Outgoing Data	Uptime
172.20.120.222-172.20.120.222	Bring Down	552 B	0 B	3 seconds



Level	Action	Status	
	negotiate	success	negotiate IPsec phase 2
	negotiate	success	progress IPsec phase 2
	tunnel-up		IPsec connection status chan
	phase2-up		IPsec phase 2 status change
	install_sa		install IPsec SA
	negotiate	success	progress IPsec phase 2
	negotiate	success	progress IPsec phase 1
	negotiate	success	progress IPsec phase 1
	negotiate	success	progress IPsec phase 1
	negotiate	success	progress IPsec phase 1

Select an entry to view the connection details, including **IPSec Local IP**, **IPSec Remote IP**, **VPN Tunnel** type, **User**, and more.

The **IPSec Remote IP** shown here should match the **Remote Gateway** shown under **VPN > Monitor > IPsec Monitor**.



Action	negotiate	**Cookies**	ba6132a63bde0998/b8f7fc6b07cdc7bb
Date/Time	13:13:15 (1380805995)	**ESP Auth**	HMAC_SHA1
ESP Transform	ESP_AES	**Group**	N/A
IPSec Local IP	172.20.120.81	**IPSec Remote IP**	172.20.120.222
Level	notice	**Local Port**	500
Log ID	37122	**Message**	negotiate IPsec phase 2
Outgoing Interface	wan1	**Remote Port**	500
Role	responder	**Status**	success
Sub Type	vpn	**Timestamp**	Thu Oct 3 13:13:15 2013
User	bwayne	**VPN Tunnel**	L2TP
Virtual Domain	root	**XAUTH Group**	N/A
XAUTH User	N/A		